INFORMATION AND CONTROL 4, 364–370 (1961)

A Note on a New Class of Codes

GUSTAVE SOLOMON

Lincoln Laboratory, Massachusetts Institute of Technology, Lexington 73, Massachusetts*

Error correcting codes of all (k, p) group codes (p odd), i.e., linear mappings of k-tuples of zeros and ones into p-tuples of zero and ones, are viewed as a purely algebraic problem. This problem concerns the zeros of certain polynomials on pth roots of unity. These polynomials are parameterized via elements of subgroups of the smallest field containing the pth roots of unity.

We introduce, in addition, the so-called jump-shift register codes. These are $((p + 1)/2, p)$ single error-correcting codes for p, a prime for which 2 has multiplicative order $p - 1$. These noncyclic codes are placed in a pseudo-cyclic setting and are easily encodable and decodable.

I. INTRODUCTION

In their treatment of Bose-Chaudhuri codes, Mattson-Solomon (1961) have introduced a new way of looking at all cyclic codes. To every code word of odd length p is associated a certain polynomial. The components of the code vector are just the values taken by this polynomial on the pth roots of unity. Error correction properties of the codes are translated into finding roots of polynomials on the pth roots of unity. This approach has yielded some interesting new results for cyclic codes, and Bose-Chaudhuri codes in particular.

We apply the new approach to all group codes and re-examine the problem in this context. We thus establish an isomorphism between all group codes and subgroups of direct products of certain fields, and using this approach obtain a new set of codes—pseudo-cyclic codes. These are codes for certain primes $p \equiv \pm 3$ modulo 8 for which 2 has order $p - 1$ which are obtained using shift register techniques. These are analogous to certain Bose-Chaudhuri $((p + 1)/2, p)$ codes, e.g., (12, 23), (9, 17), and (24, 47).

* Operated with support from the U.S. Army, Navy, and Air Force.

II. GENERAL REPRESENTATION OF GROUP CODES

Let us consider $V_p(F)$, the vector space of dimension p(odd) over the field[1] F of two elements 0 and 1. To every $a = (a_0, a_1, \cdots a_{p-1}) \in V_p(F)$ we associate a polynomial $g_a(x)$ of degree less than or equal to $(p-1)$ such that $g_a(\beta^i) = a_i$ where β is a primitive pth root of unity. (We choose $g_a(x) = 0$ for $a = (0, 0, \cdots 0)$.) The condition that $g_a(x) = 0$ or 1 for $x = \beta^i$, $i = 0, 1, \cdots p-1$, leads us, assuming

$$g_a(x) = \sum_{i=0}^{p-1} c_i x^i,$$

to $g_a(x)^2 = g_a(x)$. For $x = \beta^i$,

$$\sum_{i=0}^{p-1} c_i^2 x^{2i} = \sum c_i x^i.$$

We have thus $\sum_{i=0}^{p-1} (c_i^2 + c_{2i}) x^{2i} = 0$ for $x = \beta^i$, where all powers of x are reduced modulo p. This leads to the condition on the c_i :

$$c_0^2 = c_0, \qquad c_i^2 = c_{2i}, \qquad i = 1, 2, \cdots p-1.$$

Note that we have a form for $g_a(x)$ which involves very few independent constants. These are $c_0 \in F$ and $c_{l_1}, c_{l_2}, \cdots c_{l_{r-1}}$ where c_{l_i} is not conjugate to c_{l_j} for $l_i \neq l_j$, i.e., $c_{l_j} \neq c_{l_i}^{2^s}$ for some s.

We may actually express the c_i explicitly in terms of the components a_i and the pth roots of unity. Using a previously obtained result (Reed-Solomon, 1959) we have[2]

$$c_k = \sum_{i=0}^{p-1} a_i (\beta^i)^{-k}.$$

We see that

$$c_0 = \sum_{i=0}^{p-1} a_i, \qquad c_1 = \sum_{i=0}^{p-1} a_i \beta^{-i}, \qquad c_2 = c_1^2, \qquad c_4 = c_1^4, \cdots.$$

[1] Instead of F, we may choose any finite field, say $L = GF(q^m)$ (the Galois field of q^m elements) and stipulate that p and q be relatively prime. We thus obtain from the equation

$$g_a(x)^{q^m} = g_a(x)$$

conditions on the c_i, and establish an analogous representation for $V_p(L)$.

[2] Outline of proof: Let $g(x) = \sum_{i=0}^{m} c_i x^i$, $m < p$. Then $c_k = \sum g(x) x^{-k}$ where the summation is over the pth roots of unity. Evaluate $g(x)$ in the formula for c_k, i.e., $c_k = \sum [\sum c_i x^i] x^{-k}$, interchange the order of summation, and use the fact that $x^p + 1 = (x+1)(\sum_{i=0}^{p-1} x^i) = 0$, p an odd prime.

It is clear that the c_i are in the smallest field K over F containing the pth roots of unity.

Clearly, if we make correspond to every $a \in V_p(F)$ a set of elements of K of the form $(c_0, c_1, c_{i_1}, c_{i_2}, \cdots c_{i_r})$ where $c_0 = 0$ or 1 depending on the parity of the total number of ones in the vector a, and c_1 is the coefficient of x, c_{i_1} is the coefficient of x^{i_1}, where i_1 is the smallest integer such that $i_1 \neq 2^s(p)$ for any s, i_2 is the smallest integer larger than i_1 such that $i_2 \neq 2^s$ or $i_2 \neq i_1 2^s(p)$, etc. The correspondence $a \rightarrow (c_0, c_1, c_{i_1}, c_{i_2}, \cdots c_{i_{r-1}})$ is an additive isomorphism (depending on the initial choice of β) between $V_p(F)$ and a subgroup of the direct product of F with r copies of $K(F \times K^r)$. If p is a prime, then $V_p(F)$ is exactly isomorphic to $F \times K^r$.

If φ is a mapping of $V_k(F)$ into $V_p(F)$, then there is clearly a subgroup of this direct product which corresponds to $\varphi(V_k)$. The elements of $\varphi(V_k)$ are the values taken by $g_a(x)$ over the pth roots of unity. The polynomial $g_a(x)$ is given very simply by

$$g_a(x) = c_0 + \sum_{j=1}^{0(2)-1} (c_1 x)^{2^j} + \sum_{k=1}^{r-1} \sum_{j=0}^{0(i_k)-1} (c_{i_k} x^{i_k})^{2^j}$$

where $0(i)$ is the smallest integer m_i such that $i2^{m_i} \equiv 1$ modulo p.

Some values of r are $r(7) = 2$, $r(13) = r(11) = 1$, $r(31) = 6$. The Bose-Chaudhuri codes arise when $r(n) \geqq 2$. They are obtained naturally from setting some of the $c_i = 0$. There is a natural difference equation and polynomial associated with this mapping and these codes are generated by a shift register (Solomon, 1960).

We observe parenthetically that r depends on the multiplicative order k of 2 modulo p, i.e., k is the smallest integer such that $2^k = 1$ modulo p. This determines the number of conjugates a primitive pth root of unity will have and hence the degree of the polynomial (and/or the difference equation) which will generate the code. r is, of course, the number of irreducible factors of $(x^p + 1)/(x + 1)$ over F. A full discussion of these matters including a detailed analysis of the primes where $r = 2$ is to be found in "A New Treatment of Bose-Chaudhuri Codes" (Mattson, Solomon, 1961).

For certain p congruent to ± 3 modulo 8, $r(p) = 1$. This means that the irreducible factors of $x^p + 1$ are $(x + 1)$ and $(1 + x + x^2 + \cdots x^{p-1})$. It is for these p that we construct a new classs of codes. Certain values of such p are $p = 11, 13, 29, 19$, etc. Not all $p \equiv \pm 3$ (modulo 8) have this property, i.e., for $p = 43$, 2 has order 14, $r(p) = 3$, and for $p = 157$, 2 has order (52), $r(p) = 3$.

III. ERROR CORRECTING PROPERTIES

A (k, p) group code is r error correcting (or detecting) if $r = [d/2]$,[3] d odd (d even) where d is the minimum weight of all nonzero vectors in $\varphi(V_k) \subset V_p$; d = the smallest total number of ones in any $a \neq 0$ in $\varphi(V_k)$. Clearly, d is equal to the minimum number of ones taken on by $g_a(x)$ as $a \neq 0$ runs through $\varphi(V_k)$. This is p—maximum number of zeros of $g_a(x)$ (for any a) as x runs through the pth roots of unity. The error correcting property of any code is actually an algebraic property of polynomials of this special form: What is the maximum number of zeros $g_a(x)$ can have on the pth roots of unity?

The interesting fact here is that all group codes can be placed in this setting and all coding problems can be looked upon in this more algebraic light. Clearly, the determination of the zeros of these $g_a(x)$ may not be a simple one, but we can certainly let the c's run through a subgroup of K and compute $g_a(\beta^i)$ for such c very handily.

IV. A NEW CLASS OF CODES

A. Jump-Shift Register Codes

We now consider a hitherto hard-core class of codes. These are the noncyclic (k, p) codes for p prime of the form $8l \pm 3$ and $r(p) = 1$. The cyclic codes for these p are the simple $(1, p)$, $(p - 1, p)$ codes with known error correcting properties. They are generated by difference equations associated to the polynomials $(x + 1)$ or $(1 + x + x^2 + \cdots x^{p-1})$. If we are searching for (k, p) codes, $k \neq 1$, $k \neq p - 1$, we must rely on the old methods of generating them. We must find linear transformations T which map $V_k(F)$ into $V_p(F)$.

We shall generate new codes still employing the shift register device that generates sequences but we don't shift in the usual way; we shall jump shift the register and employ the values thus obtained differently. We are going to search for a new class of codes which are single error correcting. Our results are:

> There is a class of codes which send $(p + 1)/2$ bits into p bits which are at least single error correcting. These codes are generated using the shift register device for $(p - 1)$ length code words in a simple manner.

[3] $[d/2]$ denotes the largest integer $\leqq d/2$.

B. The Codes

Let p be a prime of type $r(p) = 1$, e.g., 11, 13. Then for β, a primitive pth root of unity, and any $a = (a_0, a_1, \cdots a_{p-1}) \in V_p(F)$, we associate the polynomial $g_a(x)$

$$g_a(x) = c_0 + cx + c^2x^2 + c^4x^4 + \cdots c^{2^{(p-1)/2}}x^{p-1} + c^{2^{(p+1)/2}}x^{p-2} + \cdots c^{2^{p-2}}x^{(p+1)/2}$$

such that $g_a(\beta^i) = a_i \in F$. As noted above

$$c_0 = \sum_{c=0}^{p-1} a_i = \text{weight of } a \text{ modulo 2 and } c = \sum_{c=0}^{p-1} a_i\beta^{-i}.$$

Observe that for $c = 0$, we obtain either the all-zero or all-one vector. For $c = 1$, $c_0 = 1$, we obtain $\sum_{i=0}^{p-1} x^i$ which is 0 for $x = \beta^i$, $i = 1, \cdots p - 1$. For such a pair (1, 1), we obtain a vector of weight one. For $c = \beta^k$ and $c_0 = 1$, our zeros are $x = \beta^i$, $i = 0, \cdots p - 1$ $i \neq k$. Thus, as c runs through the powers of β^i, we obtain all possible vectors of weight one.

To insure single error correcting, $g_a(x)$ must have at most $(p - 3)$ zeros on the pth roots of unity. We shall choose a set of c's to insure this happening. We rewrite $g_a(x)$ in descending powers of x

$$g_a(x) = c^{2^{(p-1)/2}}x^{p-1} + c^{2^{(p+1)/2}}x^{p-2} + \cdots + cx + c_0.$$

To eliminate vectors of weight one, we stipulate that $c^p \neq 1$ as above.

For $g_a(x)$ to have $(p - 2)$ zeros on pth roots of unity, we recognize immediately that $c_0 = 0$ since the weight of such vectors is 2. Now the product of the nonzero roots of $g_a(x)$ is given by $c/c^{2^{(p-1)/2}}$ or $c^{(2^{(p-1)/2}-1)-1}$. Since these are all supposed to be pth roots of unity, then their product must satisfy $c^{(2^{(p-1)/2}-1)p} = 1$. Thus, if we choose a subgroup C of $GF(2^{p-1})$ of the elements c,

$$c \in C \ni c^{(2^{(p-1)/2}-1)p} \neq 1,$$

the code (c_0, c), $c_0 \in F$, $c \in C$ will be a single error correcting code of dimension $(\dim C + 1)$. We shall now choose C for $p = 8n \pm 3$ in such a way that $\dim C = (p - 1)/2$.

The field K which contains the pth roots of unity for this p has the form $GF(2^{p-1})$, i.e., $(p - 1)$ is the degree of the smallest irreducible polynomial $f(x) = 1 + x + x^2 \cdots + x^{p-1}$ which has β as a root. The field $K = GF(2^{p-1})$ has subfields, as we shall see very clearly. For $p = 8n + 3$, $GF(2^{p-1})$ contains subfields of degree 2 and $4n + 1$ over F.

Let α be a generator of the multiplicative group K^* of $GF(2^{p-1}) = K$, i.e., $K^* = \alpha^i$, $i = 0, \cdots, 2^{p-1} - 1$. We notice now that if $\beta = \alpha^{2^{4n+1}+1}$, then the powers of β are a multiplicative group of order $2^{4n+1} - 1$ and therefore must be in the subfield of $K \cong GF(2^{4n+1})$ which is of degree $4n + 1$ over F. Choose $\gamma = \alpha^{(2^{p-1}-1/3}$ a cube root of unity and incidentally in $GF(2^2)$. The set $C = \gamma GF(2^{4n+1})$ is thus an additive subgroup of $GF(2^{p-1})$ and has the obvious property that

$$C^{(2^{(p-1)/2}-1)p} \neq 1.$$

For $p = 8n + 5$, we note that $GF(2^{8n+4})$ has subfields of order 4 and $2n + 1$, and, proceeding as before, we choose γ a fifth root of unity $= \alpha^{(2^{p-1}-1)/5}$ and let $C = \gamma GF(2^{4n+2})$. The code words associated with the pair (c_0, c), $c_0 \in F$, $c \in C$ will yield a $((p + 1)/2, p)$ code which is at least single error correcting.

We observe here the parallel to the $((p + 1)/2, p)$ Bose-Chaudhuri codes where $r(p) = 2$. There is a one-to-one correspondence between each p letter word and the tuple (c_0, c) where $c_0 \in F$ and $c \in GF(2(p - 1)/2)$. These codes turn out to be at least one error correcting and are usually much more. The (12-23) Golay code is 3-error correcting and the (24-47) code is at least 3-error correcting. The error correction properties of these cyclic codes seem to depend as much on the magnitude of p as on its congruence position relative to 8. It seems that these pseudo-cyclic $((p + 1)/2, p)$ codes will in general be more than single error correcting. The full error correcting properties have as yet to be investigated.

For n-error correcting codes we must establish more criteria on the C. Once sufficient criteria are established, we may actually form the necessary subgroups and encode.

C. Encoding

We present a possible nonsystematic method of encoding. We wish to encode the vectors $(g_c(\beta^i))$ for $g_c(x) = c_0 + cx + c^2x^2 + \cdots c^{2^{(p-1)/2}}x^{p-1}$ where $c \in \{\gamma GF(2^{(p-1)/2}), \gamma^3 = 1$ for $p \equiv 3$ (modulo 8); $\gamma^5 = 1$ for $p = -3$ (modulo 8), $c_0 \in F\}$. Let α be a $(p - 1)$ length sequence of zeros and ones which generates $V_{p-1}(F)$ via the shift register Bose-Chaudhuri encoding procedure. We form the matrix $B = (b_{ij})$, $b_{ij} = (\beta^i)^{2^{j-1}}$, $i = 0, 1, \cdots p - 1, j > 0$ where $\beta = \alpha^{2^{(p-1)/2}+1}$, $b_{i,0} = 1$. The powers of β are obtained by shifting the register $2^{(p-1)/2} + 1$ times. We jump-shift the register, so to speak.

The code words of length $a = (a_0, a_1, \cdots a_{p-1})$ are obtained very simply by applying the matrix B to the column vector $\mathbf{c} = [c_0, c, c^2, \cdots c^{2^{p-1}}]$. These operations can be done in the shift register device employed for length $p - 1$. $B\mathbf{c}$ is a column vector of length p whose entries are zeros and ones.

The information bits to be translated, i.e., $(x_0, x_1, \cdots x_{(p-1)/2})$ corresponds to

$$c_0 = x_0 \qquad c = \gamma \sum_{i=1}^{(p-1)/2} x_i \delta_i \in GF(2^{(p-1)/2}),$$

δ_i a basis for $GF(2^{(p-1)/2})$. We translate $(x_0, x_1, \cdots x_{(p-1)/2})$ into c_0, and c by keeping c_0 and generate c by the shift register. (We can very simply translate $x_1, \cdots x_{(p-1)/2}$ as that power of δ corresponding to the binary number represented by $(x_1, x_2, \cdots x_{(p-1)/2})$ using for δ a primitive element of $GF(2^{(p-1)/2})$).

D. Decoding

If an error is made in transmission, we receive $(g_{c'}(\beta^i))$ where $c' = c + \beta^k$ indicating an error was made in the kth coordinate. To compute c from $c' = \sum_{i=0}^{p-1} a_i' \beta^{-i}$, simply shift the register that power of β which when added to c' yields an element of C. This is unique. We also add 1 to the computed value of $c_0' = \sum a_i'$, since one error was made in transmission. The decoding technique here is identical to that used in Bose-Chaudhuri codes (Peterson, 1961).

This class of single error correcting codes serves as an interesting example of some of the possible uses involved in introducing a multiplication on vector spaces over F. For p where $r(p) \geqq 2$ we may use Bose-Chaudhuri or pseudo-cyclic modifications of such.

References

Mattson, H. F., and Solomon, G. (1961). A new treatment of Bose-Chaudhuri codes. To appear in *J. Soc. Ind. Appl. Math.*

Peterson, W. W. (1961). "Error Correcting Codes," Chapter 9 (9.5, 9.6). MIT and Wiley, New York.

Reed, I. S., and Solomon, G. (1959). Decoding procedure for a polynomial code. Group Report 47.24, Lincoln Laboratory.

Solomon, G. (1960). Linear recursive sequences as finite differences equations. Group Report 47.37, Lincoln Laboratory.